Displaced Person Identity Without Documents

by Nick Clark | Published March 27, 2026 | PDF

Over one hundred million people worldwide are forcibly displaced, and many have lost every document that proves who they are. Without identity, they cannot access services, cross borders legally, or rebuild their lives. Keyless identity provides a structural mechanism for identity that does not depend on documents, government databases, or biometric enrollment, building instead from accumulated behavioral continuity that begins from the moment of first contact with humanitarian systems.

The identity void in displacement

When people flee conflict, disaster, or persecution, identity documents are among the first casualties. Birth certificates, national IDs, and passports are destroyed, confiscated, or left behind. The government that issued those documents may no longer exist, may refuse to cooperate, or may be the entity the

person is fleeing from. The person's identity, as far as the international system is concerned, disappears.

Without identity, displaced persons cannot register for asylum, access healthcare, enroll children in school, open bank accounts, or obtain legal employment. Identity is not a convenience. It is the prerequisite for every other right and service. The loss of identity documents creates a compounding vulnerability that traps displaced persons in a cycle of exclusion.

Current humanitarian identity systems attempt to fill this gap through registration processes that create new identifiers and link them to biometric data. These systems provide genuine value but face structural limitations: they depend on enrollment infrastructure that may not be available in crisis zones, they create centralized databases that present surveillance and breach risks for vulnerable populations, and they produce identities that are only recognized within the issuing organization's systems.

Why biometric enrollment creates risks for vulnerable populations

Biometric enrollment of displaced persons creates stored templates in databases controlled by international organizations or host governments. For populations fleeing persecution, the existence of these databases creates risks that may outweigh the benefits. A biometric database of members of a persecuted ethnic group, if accessed by the persecuting government, becomes a targeting tool. A database of asylum seekers, if breached, can be used for identity theft or exploitation.

The consent model for biometric enrollment in displacement settings is structurally compromised. A person who needs food, shelter, and legal protection cannot meaningfully consent to biometric capture when the alternative is denial of services. The power imbalance renders the consent nominal rather than genuine.

Furthermore, biometric identities issued by one organization are typically not portable to other organizations or to the host country's identity system. A UNHCR registration does not automatically translate into recognized identity in the host country. The displaced person may need to re-enroll with multiple organizations and multiple government agencies, each creating its own stored biometric template.

How keyless identity addresses this

Keyless identity begins building from the moment of first contact with any system, without requiring enrollment infrastructure, biometric capture, or centralized databases. The person's identity emerges from their accumulated interactions: registration conversations, medical encounters, food distribution events, shelter assignments, and interactions with humanitarian workers. Each interaction extends a dynamic hash chain anchored in the specific circumstances of that interaction.

The trust slope strengthens with each legitimate interaction. A person who has been receiving services at a camp for six months has an accumulated behavioral trajectory that an impersonator cannot replicate. The identity does not depend on what the person carries or what a database contains. It depends on the consistency of the person's accumulated interactions over time.

No centralized database of identities is created. The trust slope is distributed across the interactions themselves. There is no single database to breach, no stored template to steal, and no enrollment record that could be used for surveillance. The identity is structurally resistant to the specific threats that displaced populations face.

What implementation looks like

A humanitarian deployment of keyless identity integrates trust slope generation into existing service delivery touchpoints. When a displaced person receives food, medical care, or legal assistance, the interaction contributes to their accumulating trust slope. No additional enrollment step is required. The identity builds naturally through the services the person already receives.

For cross-organizational recognition, the trust slope provides a portable identity mechanism. When a person registered with one humanitarian organization needs services from another, the accumulated trust slope provides a basis for identity validation without requiring re-enrollment or database sharing between organizations. Each organization evaluates the trust slope against the person's current behavioral signals.

For host country integration, the accumulated trust slope provides a foundation for formal identity establishment. A displaced person who has built a strong trust slope through years of consistent interactions with humanitarian systems has a demonstrable identity trajectory that can inform the host country's identity issuance process without requiring documents from a country of origin that cannot or will not cooperate.

For child protection, keyless identity addresses the particular vulnerability of unaccompanied minors who have no documents and no adults to vouch for them. The child's trust slope builds from their first interaction with protection services, providing an identity that persists through foster placements, relocations, and eventual family reunification or resettlement.

Keyless Identity All 21 steps →

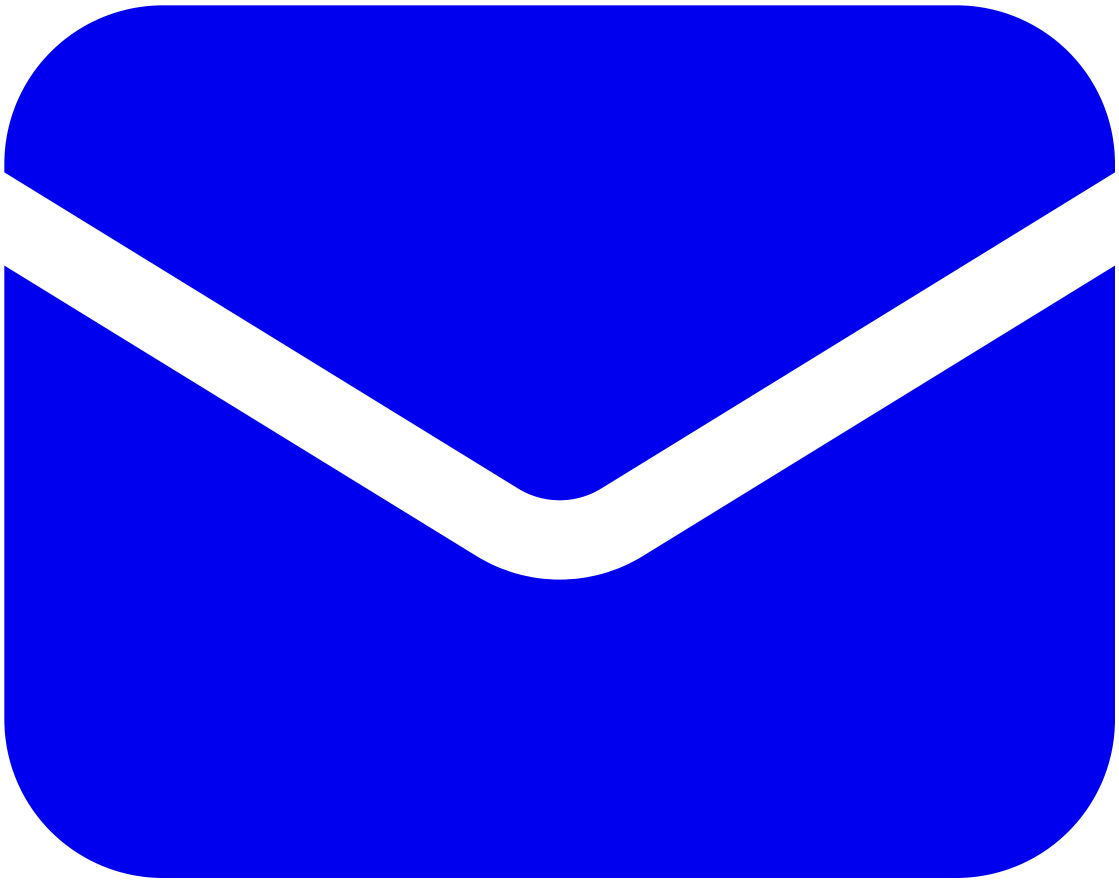
Identity from accumulated continuity. Post-quantum by construction.

Patent
US 19/388,580 · published
Primary Technical Disclosure
○ Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems
Secondary Technical
○ Continuity-Based Biological Identity Using Trust-Slope Validation○ Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials○ Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch○ Stateless Symmetric Encryption: Session Keys Derived From Current Identity State○ Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation○ Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host○ Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains○ Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification○ Quorum-Based Identity Recovery: Peer Attestation After Memory Loss○ Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links○ Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation○ Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments○ Sparse Trust

Slope Recovery: Compact Checkpoints for Resource-Constrained Devices○ Predictive Identity Validation: Drift Detection Before Full Discontinuity○ Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries○ Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions
Applications (General)
○ Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents○ Post-Quantum Enterprise Identity Migration○ Billions of IoT Devices Need Authentication Without Keys○ Financial Identity Without Credential Databases○ Patient Identity Through Behavioral Continuity○ Supply Chain Authentication Without PKI○ Smart Building Access Through Continuity○ Vehicle Operator Identity Binding● Displaced Person Identity Without Documents
Applications (Specific)
○ Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere.○ Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change.○ YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability.○ CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It.○ Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System.○ Jumio Automated ID Verification. The Verification Still Depends on Documents.○ Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.○ Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.○ OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.○ Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.○ Thales HSMs Protect Key Material. The Keys Still Exist.○ Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.○ DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits.○ Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same.
Keyless Identity overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie